(12) UK Patent Application (19) GB (11) 2 354 392 (13) A

(43) Date of A Publication 21.03.2001

(21) Application No 0005045.0

(22) Date of Filing 03.03.2000

(30) Priority Data
(31) 99039346 (32) 14.09.1999 (33) KR

(51) INT CL[7]
H04N 7/167

(52) UK CL (Edition S)
H4F FDE F13A F22 F3P F3T

(56) Documents Cited
GB 2322030 A WO 99/35647 A1 WO 99/18729 A1
WO 99/16244 A1

(58) Field of Search
UK CL (Edition R) H4F FDE FDX FGJ FGS FKX
INT CL[7] H04N 5/913 7/16 7/167
ONLINE: WPI; JAPIO; EPODOC; NPL; TDB

(71) Applicant(s)
Samsung Electronics Company Limited
(Incorporated in the Republic of Korea)
416 Maetan-dong, Paldal-gu, Suwon-city,
Kyungki-do, Republic of Korea

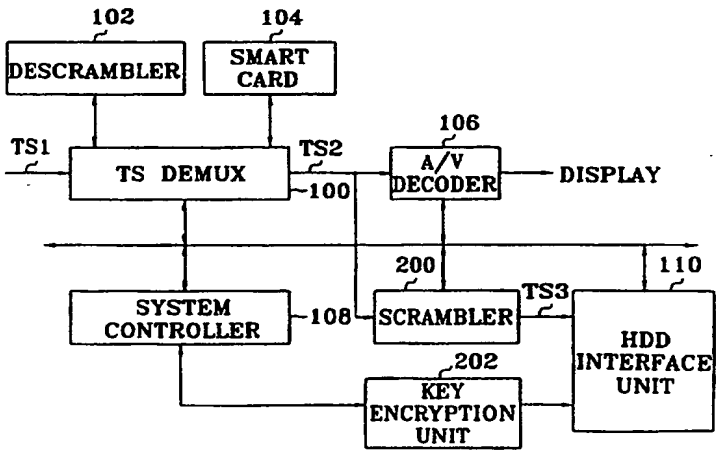
(72) Inventor(s)
Myung-Sik Yim

(74) Agent and/or Address for Service
Appleyard Lees
15 Clare Road, HALIFAX, West Yorkshire, HX1 2HY,
United Kingdom

(54) Abstract Title
Copy prevention apparatus and method in digital broadcasting receiving system

(57) A copy prevention apparatus and method in a digital broadcasting receiving system protects information stored in a storage medium from being illegally duplicated by an unauthorised third party. The copy prevention apparatus includes a demultiplexer (100) for descrambling scrambled transport stream (TS) patterned data of a user selective and desired channel among a received multi-channel broadcasting and outputting the descrambled result, a scrambler (200) for scrambling again the descrambled TS patterned data from the TS demultiplexer, a key encryption unit (202) for decrypting the encrypted key of the scrambler and re-encrypting the decrypted key again, to thereby produce a new encryption key, and a system controller (108) for controlling a storage medium to store the scrambled TS patterned data from the scrambler together with the encrypted scrambler key output from the key encryption unit during storing. Thus, the copy prevention apparatus and method in the digital broadcasting receiving system scrambles again a descrambled data stream in a specific method and stores the scrambled result, when a received broadcasting signal is stored in a storage medium such as a hard disc drive (HDD) or a DVD-RAM drive.

FIG. 2



GB 2 354 392 A

FIG. 1 (PRIOR ART)

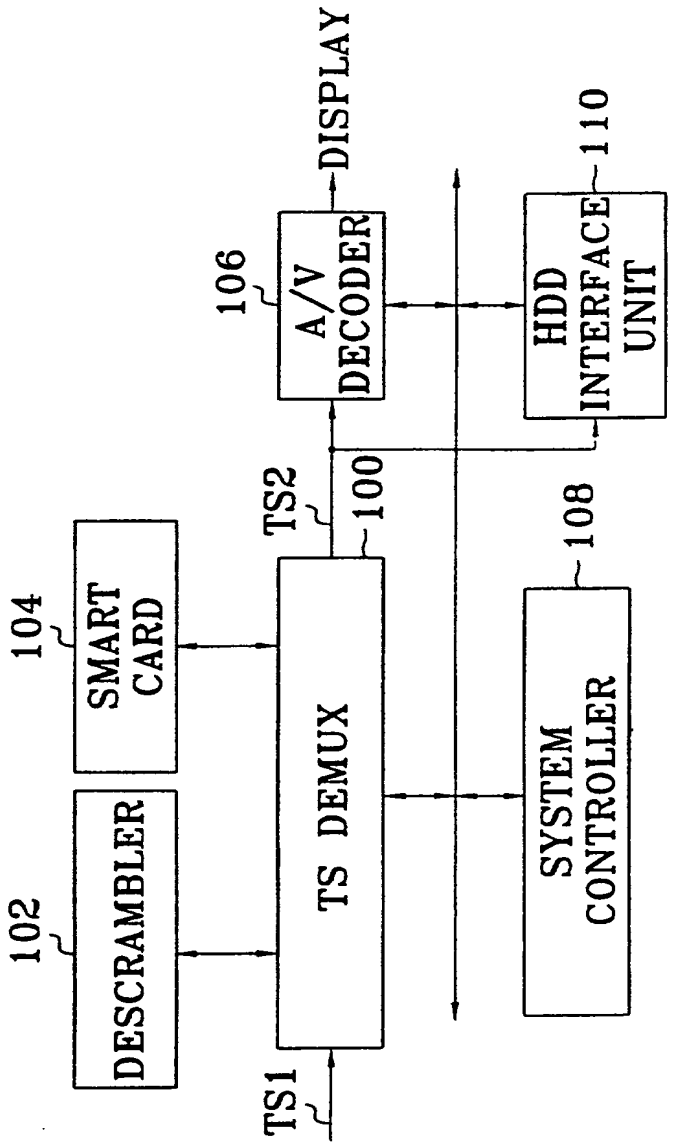


FIG. 2

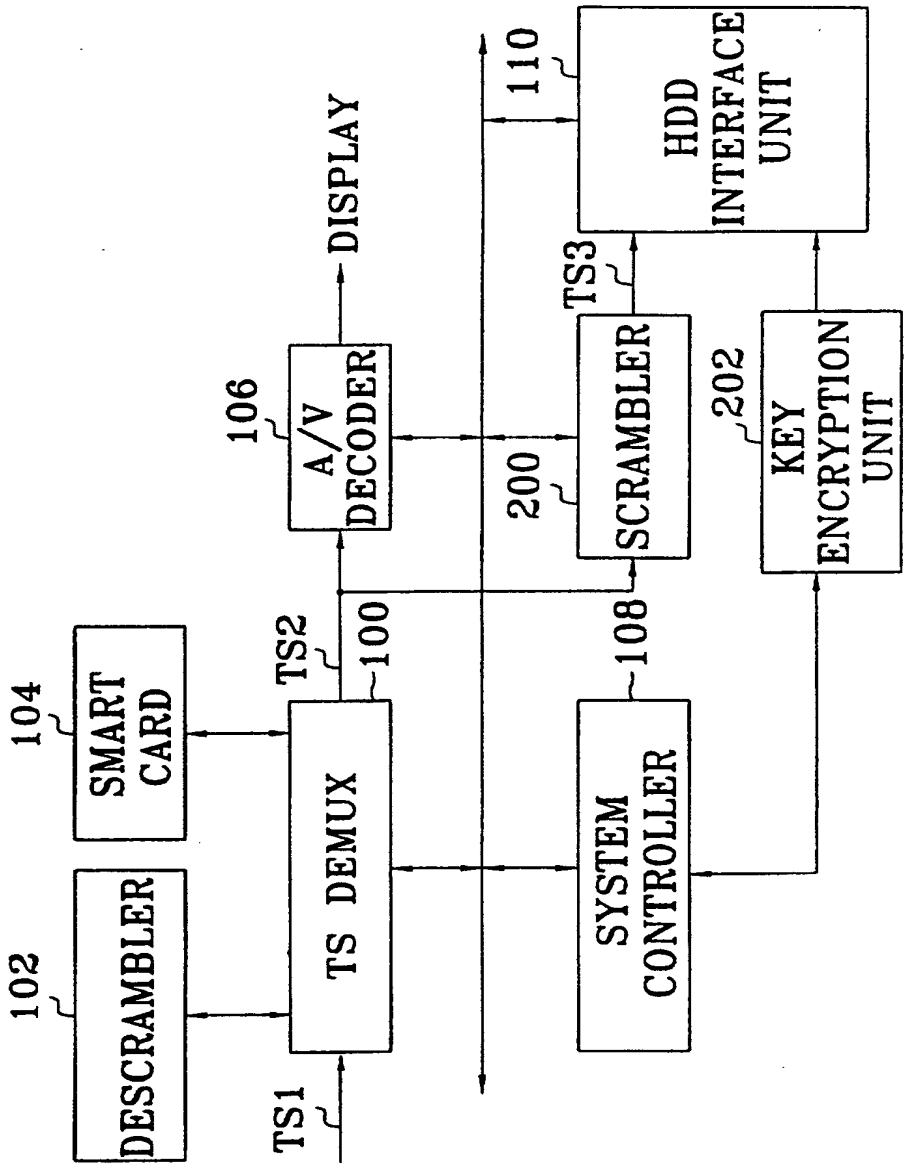


FIG. 3

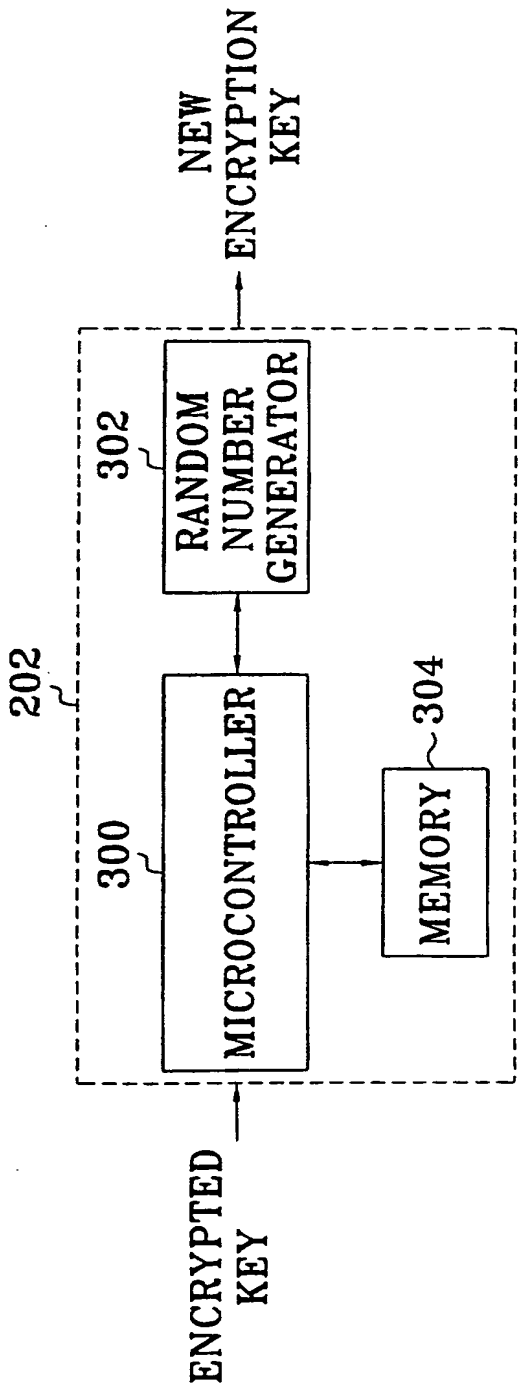
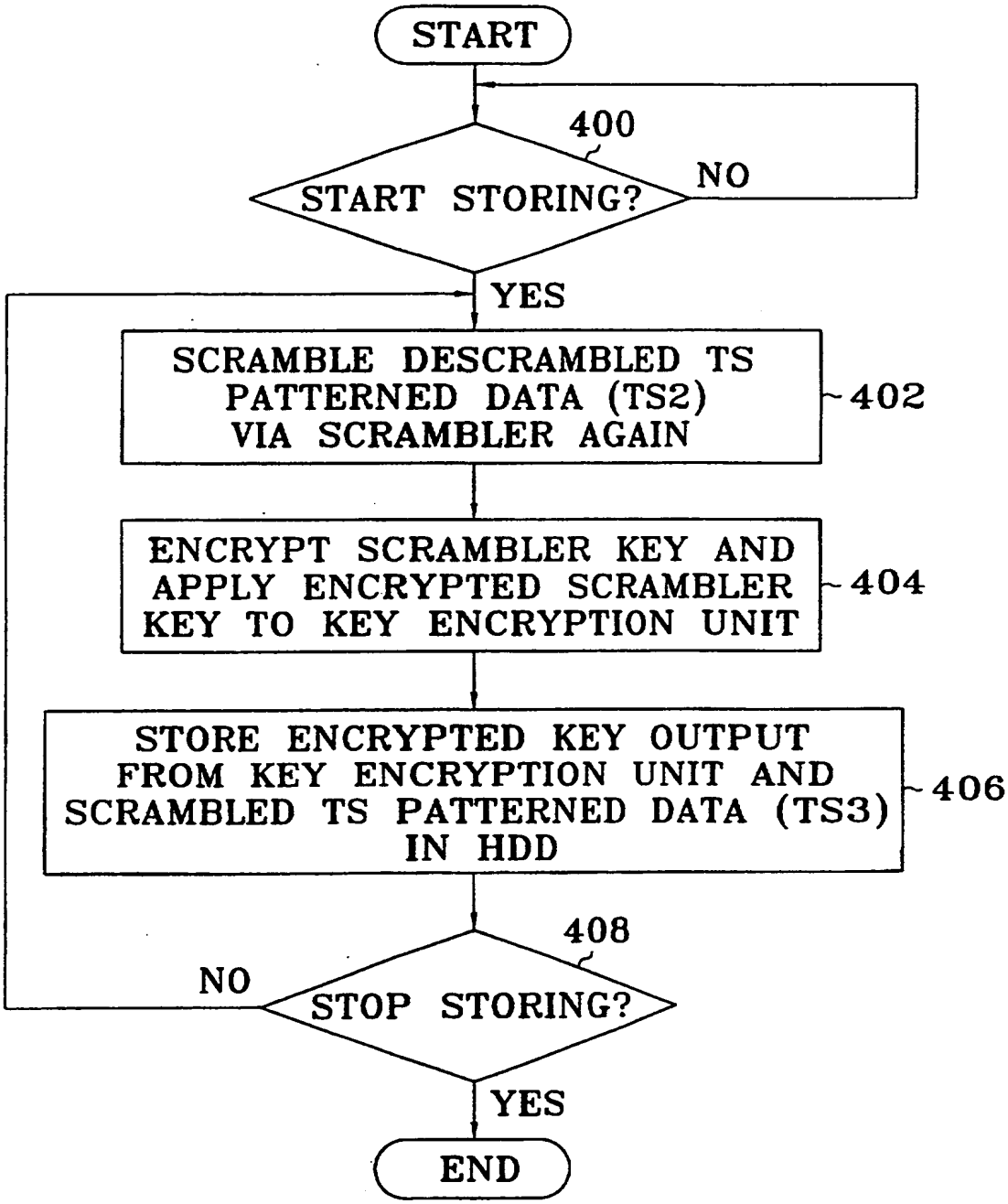


FIG. 4



COPY PREVENTION APPARATUS AND METHOD IN DIGITAL BROADCASTING RECEIVING SYSTEM

The present invention relates to a broadcasting receiving system for receiving a digital broadcasting and storing the same, and more particularly, to a copy prevention apparatus and method in a digital broadcasting receiving system in which an unauthorized illegal copy of a broadcasting signal whose copyright should be protected is prevented when the broadcasting signal is stored in a storage medium.

A hard disk drive (HDD) is an auxiliary storage device for use in computers, in which random access is possible, data transfer speed is high and its cost is lower than other auxiliary storage devices, to thereby however realize a large capacity. Recently, a digital versatile disc (DVD) is favoured as a next-generation storage medium. A recent form of the DVD is a DVD-RAM free of recording and deletion of data. Accordingly, the HDD or DVD-RAM drive is used as a storage device in a broadcasting receiving system, to thereby enable a user to view a broadcasting program or store the same.

Meanwhile, a digital broadcasting employing a multi-channel and containing a plurality of programs for each channel has started. A digital broadcasting receiving system receives multi-channel digital audio/video data transmitted via a broadcasting station or network and reproduces and stores the received data. Generally, digital audio/video data is encoded by the MPEG (moving picture expert group) standard and is transmitted in the form of a digital transport stream (TS) packetized

including data of a number of programs. Here, the data of the programs is encoded by an encryption or scramble method, and decoded only in a broadcasting receiving system where a view of programs is allowed.

The above-described prior art reference will be described in more detail with reference to Figure 1 showing a schematic structure of a broadcasting receiving system adopting a general HDD.

In Figure 1, a TS demultiplexer 100 extracts a key of an encrypted scrambler from data TS1 of an input scrambled TS pattern. The TS demultiplexer 100 decrypts a scrambler key extracted according to user information programmed in advance on a smart card 104. The decrypted scrambler key and the input TS patterned data TS1 are input to a descrambler 102. The descrambler 102 descrambles the input TS patterned data TS1 using a decrypted key applied from the TS demultiplexer 100. The descrambled TS patterned data TS2 is input to an audio/video (A/V) decoder 106 or a HDD interface unit 110 via the TS demultiplexer 100 under the control of a system controller 108 responding to a reproduction or storing request from a user. In the case that a user requests a reproduction operation, the A/V decoder 106 decodes the input descrambled TS patterned data TS2 to be displayed so that the user can view it. In the case that a user requests a storing operation, the HDD interface unit 110 stores the input descrambled TS patterned data TS2 in a HDD (not shown).

However, the above-described conventional broadcasting receiving system stores a broadcasting signal in the

descrambled form when it is stored in a storage medium. For this reason, the contents of the storage medium are copied by an unauthorised third party, in which case the stored information cannot be protected from being illegally distributed.

With a view to solve or reduce the above problems, it is an aim of embodiments of the present invention to provide a copy prevention apparatus and method for protecting stored information in a storage medium from being illegally duplicated by an unauthorised third party in which a broadcasting signal is scrambled when a broadcasting received from a digital broadcasting receiving system is stored in the storage medium.

According to a first aspect of the present invention, there is provided a copy prevention apparatus for use in a digital broadcasting receiving system for receiving a digital multi-channel broadcasting and viewing and storing a desired program, the copy prevention apparatus comprising:

a descrambler for extracting an encrypted key of a scrambler from scrambled transport stream (TS) patterned data received in correspondence to a desired channel, decrypting the extracted encrypted key, and descrambling the scrambled TS patterned data using the decrypted key;

a scrambler for scrambling the descrambled TS patterned data again;

a key encryption unit for decrypting the encrypted key of the scrambler and encrypting the decrypted key again, to thereby produce a new encryption key;

a storage medium for storing the scrambled TS patterned data together with the produced encryption key; and

a system controller for controlling the operation of each component so that data is stored after a copy prevention operation has been performed in response to a storing request from a user.

Preferably, said descrambler encrypts the decrypted key and outputs the encrypted key to the key encryption unit.

Conveniently, said key encryption unit produces an encryption key using a random number.

Alternatively, said key encryption unit produces an encryption key using a product serial number.

Preferably, said key encryption unit comprises:

a random number generator for generating a random number at the time of an initial operation;

a memory for storing the random number generated in said random number generator; and

a microcontroller for decrypting the received encrypted scrambler key, and then newly encrypting the decrypted key using the random number stored in the memory, to thereby output the newly encrypted key.

Preferably, said random number generator generates a mutually different initial value for each broadcasting receiving system, in order to prevent the data stored in the storage medium from being descrambled in other broadcasting receiving systems.

Preferably, said storage medium is a hard disc drive (HDD).

Preferably, said storage medium is a digital versatile disc-random access memory (DVD-RAM) drive.

According to a second aspect of the present invention there is provided a method for preventing a storage medium from being illegally copied in a digital broadcasting receiving system, the copy prevention method including the steps of:

(a) extracting an encrypted key of a scrambler from input scrambled transport stream (TS) patterned data;

(b) decrypting the scrambler key extracted in step (a) and descrambling the scrambled TS patterned data using the decrypted key;

(c) scrambling the descrambled TS patterned data again from step (b) in response to a storing request from a user, decrypting the encrypted scrambler key again and encrypting the decrypted key again, to thereby produce a new encryption key; and

(d) storing the scrambled TS patterned data together with the encryption key produced in step (c).

Preferably, said step (b) further comprises the step of (b1) encrypting the decrypted key again.

Conveniently, the decrypted key is encrypted to produce a new encryption key using a random number in said step (c).

Alternatively, the decrypted key is encrypted to produce a new encryption key using a system serial number in said step (c).

According to a third aspect of the present invention there is provided a broadcasting receiving system incorporating a copy prevention apparatus according to the first aspect of the present invention.

For a better understanding of the invention, and to show how embodiments of the same may be carried into effect, reference will now be made, by way of example, to the accompanying diagrammatic drawings in which:

Figure 1 is a block diagram showing a general broadcasting receiving system having a hard disc drive (HDD);

Figure 2 is a block diagram showing a broadcasting receiving system having a HDD according to a preferred embodiment of the present invention;

Figure 3 is a block diagram showing the key encryption unit of the figure 2 system; and

Figure 4 is a flow chart for explaining a copy prevention operation when data is stored in a HDD in the figure 2 system.

A preferred embodiment of the present invention will be described with reference to the accompanying drawings.

Figure 2 shows a broadcasting receiving system implementing a copy prevention function according to the preferred embodiment of the present invention. The system shown in figure 2 includes the same blocks as those of figure 1, which perform the same functions as those of the corresponding blocks in the conventional broadcasting receiving system. Here, the blocks of figure 2 have the same reference numerals as those of the corresponding blocks of figure 1. In addition, the figure 2 system according to the present invention includes a scrambler 200 positioned at the input side of a hard disc drive (HDD) interface unit 110, for scrambling the descrambled transport stream (TS) patterned data TS2 again, and a key encryption unit 202 for producing a new encryption key.

The detailed structure of the key encryption unit 202 will be described with reference to figure 3.

Figure 3 is a block diagram showing the key encryption unit 202 of the figure 2 system. The key encryption unit 202 shown in figure 3 includes a random number generator 302 for generating a random number at the time when an initial operation of the corresponding system is performed, and a memory 304 storing the generated random number. Here, the random number generator 302 has a mutually different initial value for each broadcasting

receiving system in order to prevent data stored in a hard disc drive (HDD) from being descrambled in other broadcasting receiving systems. The key encryption unit 202 of figure 3 also includes a microcontroller 300 for receiving an encrypted key of a scrambler from a TS demultiplexer 100 and decrypting the received key, and then newly encrypting the decrypted key using the random number stored in the memory 304 to thereby output the newly encrypted key. The operation of copy prevention in the digital broadcasting receiving system of figure 2 having the above constitution will be described in more detail with reference to figure 3 and figure 4.

In figure 2, if scrambled TS data TS1 is input via a network or a broadcasting station, the TS demultiplexer 100 selects a program data stream of a particular channel selected by a user among the scrambled TS data TS1 under the control of the system controller 108. The TS demultiplexer 100 transmits the selected particular channel program data stream to the descrambler 102, and then decrypts the encrypted scrambler key included in the input TS data TS1 according to user information programmed in a smart card 104 in advance, to then transmit the decrypted key to the descrambler 102. The descrambler 102 descrambles the input data stream using the decrypted scrambler key applied from the TS demultiplexer 100. The descrambled TS patterned data TS2 is supplied to an audio/video (A/V) decoder 106 and a scrambler 200 via the TS demultiplexer 100, respectively. The A/V decoder 106 decodes the descrambled TS patterned data TS2 supplied under the control of the system controller 108, to then be displayed on a display (not shown). Accordingly, the user

can view a program with respect to a certain channel which is desired to be viewed.

Meanwhile, the scrambler 200 scrambles the descrambled TS patterned data TS2 supplied under the control of the system controller 108 once again, and supplies the scrambled TS patterned data TS3 so as to be stored in a HDD via the HDD interface unit 110. Here, the scrambler 200 uses a specific scrambler of a corresponding broadcasting receiving system manufacturer, in which a product serial number is used as a scrambler key. The key encryption unit 202 decrypts an encryption key applied from the TS demultiplexer 100 via the system controller 108, and then encrypts the decrypted key using the product serial number, to thereby produce a new encryption key. Although the encrypted scrambler key extracted from the TS demultiplexer 100 may be supplied to the key encryption unit 202 without any modification, the encrypted key can be exposed during transmission. For this reason, the decrypted key is encrypted again in the key encryption unit 202. The key encryption unit 202 may use a random number instead of a product serial number. That is, as shown in figure 3, the key encryption unit 202 stores, in the memory 304, the random number produced from the random number generator 302 at the time of the system initial operation. The microcontroller 300 in the key encryption unit 202 receives the encrypted scrambler key from the TS demultiplexer 100 and then decrypts the received scrambler key, and then encrypts the decrypted key again using the random number stored in the memory 304, to produce a new encryption key. The new encryption key is stored in the HDD via the HDD interface unit 110, together with the newly scrambled TS patterned data TS3. Accordingly, the

user protects a copyright with respect to the program of the channel desired to be stored, so that the program can be stored. This operation will be described in more detail below. If a user inputs a storing command for storing a program desired to be stored, the system controller 108 performs a set of control operations in order to store data of the requested program desired to be stored in the HDD in response to the storing command. That is, as shown in figure 4, the system controller 108 performs a HDD copy prevention control operation in order to protect the information stored in the HDD when data is stored in the HDD, from being copied by an unauthorised third party.

Figure 4 is a flow chart for explaining a copy prevention operation when data is stored in a HDD in the figure 2 system. In figure 4, the system controller 108 judges whether a storing operation starts according to an input of a storing command (step 400). If a storing operation has started in the result of the step 400 judgement, the system controller 108 controls the scrambler 200 to scramble again the TS patterned data TS2 of a corresponding program which has been descrambled and output from the TS demultiplexer 100 (step 402). Then, the system controller 108 encrypts the scrambler key by software and applies the encrypted result to the key encryption unit 202 (step 404). Here, a direct one-to-one correspondence relationship between the encrypted key produced from the key encryption unit 202 and a non-encrypted key prior to being applied to the key encryption unit 202 can be exposed when the key is applied from the system controller 108 to the key encryption unit 202 without being encrypted again. Thus, the reason why the

newly encrypted key is applied to the key encryption unit 202, is for preventing a direct one-to-one correspondence relationship between the encrypted key produced from the key encryption unit 202 and a non-encrypted key prior to being applied to the key encryption unit 202 from being exposed. Accordingly, the key encryption unit 202 decrypts the encrypted key and then encrypts the decrypted key again to thereby produce a newly encrypted key. Then, the system controller 108 stores the encrypted key output from the key encryption unit 202 and the TS patterned data TS3 of a corresponding program scrambled in the scrambler 200 in the HDD via the HDD interface unit 110 (step 406). That is, the scrambler 200 scrambles the descrambled TS patterned data TS2 output from the TS demultiplexer 100 once again prior to being stored in the HDD. Then, the system controller 108 checks whether a storing stop command is input via a key inputter or a remote controller from the user (step 408). If there is no input storing stop command in step 408, the system controller 109 returns to step 402 and performs operations of the preceding steps 402-406, and scrambles the corresponding program TS patterned data TS2 and newly encrypts the scrambler key to then be stored in the HDD. Reversely, if a storing stop command has been input in step 408, the system controller 108 finishes the storing operation.

As described above, the copy prevention apparatus and method in the digital broadcasting receiving system according to the present invention scrambles again a descrambled data stream in a specific method and stores the scrambled result, when a received broadcasting signal is stored in a storage medium such as a HDD or a DVD-RAM drive, to thereby provide an effect of preventing an

unauthorised person from copying the information stored in the storage medium.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extend to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

CLAIMS

1. A copy prevention apparatus for use in a digital broadcasting receiving system for receiving a digital multi-channel broadcasting and viewing and storing a desired program, the copy prevention apparatus comprising:

a descrambler for extracting an encrypted key of a scrambler from scrambled transport stream (TS) patterned data received in correspondence to a desired channel, decrypting the extracted encrypted key, and descrambling the scrambled TS patterned data using the decrypted key;

a scrambler for scrambling the descrambled TS patterned data again;

a key encryption unit for decrypting the encrypted key of the scrambler and encrypting the decrypted key again, to thereby produce a new encryption key;

a storage medium for storing the scrambled TS patterned data together with the produced encryption key; and

a system controller for controlling the operation of each component so that data is stored after a copy prevention operation has been performed in response to a storing request from a user.

2. The copy prevention apparatus according to claim 1, wherein said descrambler encrypts the decrypted key and outputs the encrypted key to the key encryption unit.

3. The copy prevention apparatus according to claim 1 or claim 2, wherein said key encryption unit produces an encryption key using a random number.

4. The copy prevention apparatus according to claim 2, wherein said key encryption unit produces an encryption key using a product serial number.

5. The copy prevention apparatus according to claim 3, wherein said key encryption unit comprises:

a random number generator for generating a random number at the time of an initial operation;

a memory for storing the random number generated in said random number generator; and

a microcontroller for decrypting the received encrypted scrambler key, and then newly encrypting the decrypted key using the random number stored in the memory, to thereby output the newly encrypted key.

6. The copy prevention apparatus according to claim 5, wherein said random number generator generates a mutually different initial value for each broadcasting receiving system, in order to prevent the data stored in the storage medium from being descrambled in other broadcasting receiving systems.

7. The copy prevention apparatus according to any of the preceding claims, wherein said storage medium is a hard disc drive (HDD).

8. The copy prevention apparatus according to any of claims 1 to 6, wherein said storage medium is a digital versatile disc-random access memory (DVD-RAM) drive.

9. A method for preventing a storage medium from being illegally copied in a digital broadcasting receiving system, the copy prevention method including the steps of:

(a) extracting an encrypted key of a scrambler from input scrambled transport stream (TS) patterned data;

(b) decrypting the scrambler key extracted in step (a) and descrambling the scrambled TS patterned data using the decrypted key;

(c) scrambling the descrambled TS patterned data again from step (b) in response to a storing request from a user, decrypting the encrypted scrambler key again and encrypting the decrypted key again, to thereby produce a new encryption key; and

(d) storing the scrambled TS patterned data together with the encryption key produced in step (c).

10. The copy prevention method according to claim 9, wherein said step (b) further comprises the step of (b1) encrypting the decrypted key again.

11. The copy prevention method according to claim 9 or claim 10, wherein the decrypted key is encrypted to produce a new encryption key using a random number in said step (c).

12. The copy prevention method according to claim 10, wherein the decrypted key is encrypted to produce a new encryption key using a system serial number in said step (c).

13. A broadcasting receiving system incorporating a copy prevention apparatus according to any of claims 1 to 8.

14. A copy prevention apparatus substantially as herein described with reference to figures 2 to 4 of the drawings.

15. A copy prevention method substantially as herein described with reference to figures 2 to 4 of the drawings.

Application No: GB 0005045.0
Claims searched: 1-15

Examiner: Frank D. Moeschler
Date of search: 4 September 2000

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): H4F (FDE, FDX, FKX, FGJ, FGS)

Int Cl (Ed.7): H04N - 5/913, 7/16, 7/167

Other: ONLINE: WPI: JAPIO: EPODOC; TDB; NPL

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A	GB 2322030 A	(NDS)	
A	WO 99/16244 A1	(CANAL+)	
A	WO99/18729	(CANAL+)	
A	WO99/35647	(SAMSUNG)	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

BNSDOCID: <GB_____2354392A__I_>